

EXHIBIT

2

Assigned for all purposes to: Stanley Mosk Courthouse, Judicial Officer: Douglas Stern

LINDEMANN LAW FIRM, APC

Blake J. Lindemann, SBN 255747

Donna R. Dishbak, SBN 259311

433 N. Camden Drive, 4th Floor

Beverly Hills, CA 90210

Telephone: (310) 279-5269

Facsimile: (310) 300-0267

E-mail: blake@lawbl.com

Attorneys for Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES - CENTRAL DISTRICT

LINDEMANN LAW, APC, ROES 1-100,

Case No. **22STCV38451**

COMPLAINT FOR DAMAGES FOR:

Plaintiffs,

v.

RACKSPACE TECHNOLOGY, INC.; AND
DOES 1-100,

Defendants.

- 1. Intrusion Upon Seclusion**
- 2. California Constitutional Right to Privacy**
- 3. Violation of The California Confidentiality of Medical Information Act**
- 4. Violation of The California Unfair Competition Law**
- 5. Violation of The California Customer Records Act**
- 6. Violation of The California Information Practices Act**
- 7. Breach of Confidentiality**
- 8. Invasion of Privacy**
- 9. Constructive Fraud**
- 10. Breach of Express Contract**
- 11. Breach of Implied Contract**
- 12. Unjust Enrichment**
- 13. Declaratory Relief**
- 14. Negligence/Gross Negligence/Negligence Per Se**
- 15. California Consumer Privacy Act**

[Demand for Jury Trial]

LINDEMANN LAW FIRM, APC
433 N. CAMDEN DRIVE, 4TH FLOOR
BEVERLY HILLS, CA 90210

1 Plaintiffs hereby file this complaint against RACKSPACE TECHNOLOGY, INC. and DOES
2 1-100 (collectively, the “Defendants”), and demanding a trial by jury, aver as follows:

3 JURISDICTION AND VENUE

4 1. This Court has personal jurisdiction over the Defendants as they regularly transact
5 business in this judicial district.

6 2. Venue is proper in this judicial district because a substantial part of the events giving
7 rise to the causes of action occurred in this district.

8 3. This case concerns a publicized security incident perpetrated by Defendants.¹

9 4. The security incident occurred in California at Rackspace Technology’s San Jose data
10 center, which is located in San Jose, California.² Plaintiff’s data was located in Los Angeles and San
11 Jose, California.

12 THE PARTIES

13 5. Plaintiff Lindemann Law, APC is a Professional Corporation that is a citizen of
14 California.

15 6. Plaintiff Blake J. Lindemann is an individual who is a citizen of California, fdba as
16 Lindemann Law Group.

17 7. Defendant Rackspace Technology, Inc. is a publicly traded corporation, whose data
18 center is located in California. The stock price has decreased 33% since as of the writing of this
19 Complaint since the breach was disclosed.

20 8. Plaintiffs are ignorant of the true names and capacities of the Defendants DOES 1
21 through 100, inclusive, whether individual, corporate, associate, or otherwise, and therefore have
22 sued them by the foregoing names which are fictitious. Plaintiffs ask that when their true names and
23 capacities are discovered that this Complaint may be amended by inserting their true names and
24 capacities in lieu of said fictitious names, together with apt and proper words to charge them. All
25

26 ¹ <https://www.bleepingcomputer.com/news/security/rackspace-confirms-outage-was-caused-by-ransomware-attack/>.

27 ² [https://www.rackspace.com/about/data-centers/san-](https://www.rackspace.com/about/data-centers/san-jose#:~:text=Rackspace%20Technology's%20San%20Jose%20data,the%20heart%20of%20Silicon%20Valley.)
28 [jose#:~:text=Rackspace%20Technology's%20San%20Jose%20data,the%20heart%20of%20Silicon%20Valley.](https://www.rackspace.com/about/data-centers/san-jose#:~:text=Rackspace%20Technology's%20San%20Jose%20data,the%20heart%20of%20Silicon%20Valley.)

1 references to any named Defendants shall also refer to said Does. When the true names and
2 capacities are ascertained, Plaintiffs will amend this Complaint accordingly. On information and
3 belief, Plaintiffs allege that each of the fictitiously named defendants was responsible in some
4 manner for the acts and omissions alleged herein and are liable to Plaintiffs herein.

5 9. Said DOE defendants may include, but do not necessarily include, individuals,
6 businesses, corporations, partnerships, associations, joint ventures, defendants that are government
7 in nature, as well as product manufacturers, medical providers, professionals, contractors, estates,
8 administrators of estates, trusts and/or all other types of entities and/or individuals as discovery in
9 the matter may reveal. Regardless, Plaintiffs allege that each of the defendants designated herein as
10 DOE is legally responsible in some manner for the events and happenings herein referred to, and
11 legally caused injury and damages proximately thereby to Plaintiffs and each of them are alleged.

12 10. Plaintiffs are informed and believe, and based thereon allege, that each of the
13 defendants are the agent and/or employee of each and every other defendant, and in doing the things
14 herein alleged, each defendant was acting in the course and scope of said agency and/or employment
15 and that each of the acts of the defendants was ratified and confirmed by each and every other
16 defendant.

17 11. Plaintiffs are informed and believe, and based thereon allege, that each of the
18 defendants designated as a DOE is in some manner responsible for the events and happenings herein
19 referred to, and caused injury and damages proximately thereby to Plaintiffs as herein alleged.

20 **FACTS COMMON TO ALL CAUSES OF ACTION**

21 12. Defendant Rackspace Technology, Inc.'s only functionality is to provide secure and
22 accessible access to e-mails, contacts, calendars, and basic business functionalities. Instead,
23 Defendants have failed to update the most basic security and anti-cyber attack functionalities leading
24 to a massive data breach and exposure affecting Plaintiff and numerous businesses including without
25 limitation. In the aftermath, Rackspace's response has been shameful and the extent of the exposure
26 was not disclosed; instead representatives were forced to lie to consumers and were told the full
27 extent of the ransomware and exposure was not known. Not only are customers data exposed, but the
28 use of the functionality and stored data has been impossible rendering the proper functionality of

1 business to be paralyzed and causing irreparable damage and potential reputational harm due to the
2 interruption.

3 13. Plaintiff has utilized Defendant for e-mail server and exchange server services from
4 on or about 2008 to present date.

5 14. In 2022, Plaintiff reported a security incident to Defendant that involved a Rackspace
6 level infiltration and security breach to Defendant. Defendant failed to properly investigate the
7 issue. On or about 9/5/22, there was a depreciation of non-secure protocols reflected in Plaintiff's
8 customer interface. Defendants' entire business is premised on "stopping" breaches before they
9 start.

10 15. As reported by Rackspace, Cloud company Rackspace is investigating a
11 cybersecurity incident that forced it to shut down its Hosted Exchange environment. Rackspace's
12 Hosted Exchange service, which makes it easier for organizations to use Microsoft Exchange servers
13 for email, falsely claimed that it started experiencing problems on Friday, December 2. The
14 company confirmed the problems early in the day and told customers that it had to shut down the
15 Exchange environment due to what it described as "significant failure."

16 16. On Saturday, nearly 24 hours after the disruption started, Rackspace revealed that the
17 issues were caused by a "security incident".

18 17. The incident may involve exploitation of known vulnerabilities affecting Microsoft
19 Exchange, specifically CVE-2022-41040 and CVE-2022-41082, which are known as ProxyNotShell.

20 18. ProxyNotShell came to light in late September after a Vietnamese cybersecurity
21 company saw it being exploited in attacks. Microsoft confirmed exploitation and linked the
22 attacks to a nation-state hacker group. The tech giant rushed to share mitigations, but experts showed
23 that they could be easily bypassed. However, Microsoft only released patches in November.
24 Beaumont noticed that a Rackspace Exchange server cluster that is currently offline was running a
25 build number from August 2022 a few days ago. Considering that the ProxyNotShell vulnerabilities
26 were only fixed in November, it's possible that threat actors exploited the flaws to breach Rackspace
27 servers.

28 "Although the vulnerability needs authentication, the exploits work without multi-factor
authentication as Exchange Server doesn't yet support Modern Authentication at all, as

Microsoft deprioritised the implementation work,” Beaumont explained in a blog post. He added, “If you are an MSP running a shared cluster, such as Hosted Exchange, it means that one compromised account on one customer will compromise the entire hosted cluster. This is high risk.”

19. Defendants have failed to update the proxy server as required by well-known protocols.

20. Defendants have outsourced its main IT functionalities to India and other cross international domains that were unsafe and compromised Plaintiff’s information.

21. This scenario has caused chaos and disruption to over ten thousand small businesses. Twitter users have been sharing the following:

Nick Cioromski @NCioromski:

“How is the @Rackspace outage not trending? This email outage is having a catastrophic impact on small businesses all over the world and there is seemingly no end in sight. @CBSNews @FoxNews @CNN @NBCNews @ABC @WSJbusiness @CNBC”

Scott Heselmeyer @DSHeselmeyer:

“The #rackspace failure had my law firm completely shut down for 80+ hours and nearly 2 full business days. We’re up and running again and working on recovering data (luckily all of my e-mails are archived locally). Needless to say, we’ll no longer be customers.”

Sharon Jones @azsharin:

“Okay, Rackspace, this is ridiculous. I’m a small business owner unable to access my email. I have tried to reach you for an update. I finally received a call back with the “racker” laughing he had 400 more calls to return. He had absolutely no explanation. This is ridiculous.”

22. Specifically, Plaintiffs’ personal and private financial, personal, corporate, identifying, and other information has been compromised and cannot be used. Years of e-mails may have been lost, are currently inaccessible and the proposed solutions do not fix any of the problems.

23. Customers have been on hold for over 4 hours (if they can get through at all).

24. The user agreement in place does not include any arbitration provision.

25. Plaintiffs are customers of Defendants who entrusted their personally identifiable information (“PII”) and private health information (“PHI”) (together, “PII/PHI”) to Defendants.

1 Defendants betrayed Plaintiffs trust by failing to properly safeguard and protect their PII/PHI, and
2 publicly disclosing their PII/PHI without authorization, in violation of numerous laws, including,
3 *inter alia*, the California Confidentiality of Medical Information Act (“CMIA”) (Cal. Civ. Code §
4 56, *et seq.*), California Customer Records Act (“CRA”) (Cal. Civ. Code § 1798.80, *et seq.*),
5 California Unfair Competition Law (“UCL”) (Cal. Bus. & Prof. Code § 17200, *et seq.*), California
6 Information Practices Act (“IPA”) (Cal. Civ. Code § 1798, *et seq.*), and California common law.

7 26. The wrongfully disclosed and viewed PII/PHI, included, *inter alia*, Plaintiffs’ Social
8 Security number, business records, personal information, addresses, dates of birth, telephone
9 numbers, personal addresses, and personal medical information.

10 27. Defendants’ wrongful actions, inaction, and omissions directly and proximately
11 caused the Data Breach and the wrongful release and viewing of Plaintiffs’ PII/PHI to the world.

12 28. Plaintiffs are concerned about their clients, finances, credit, identities, medical
13 records, and PII/PHI and, as such, regularly monitors their credit, monitor their financial accounts
14 and/or carefully store and dispose of their PII/PHI and other documents containing their PII/PHI.
15 The concern is reasonable and justified. Because of the Data Breach, there is an immediate and
16 substantial risk of identity theft, identity fraud, medical fraud, lost medical identities and records,
17 fraudulent credit card activity, the opening or re-opening of new credit card accounts in their name,
18 phishing, increased mailers marketing products and services including, *inter alia*, medical products,
19 medical services and prescription drugs specifically targeted to their medical conditions/Plaintiff has
20 standing to bring this suit because as a direct and proximate result of Defendants’ wrongful actions,
21 inaction and omissions, and the resulting Data Breach, Plaintiffs have suffered (and will continue to
22 suffer) economic damages and other injury and harm in the form of, *inter alia*, (i) an imminent,
23 immediate and the continuing increased risk of identity theft, identity fraud and medical fraud - risks
24 justifying expenditures for protective and remedial services for which they are entitled to
25 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII/PHI, (iv) statutory
26 damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is
27 a well-established national and international market, and (vi) the financial and temporal cost of
28 monitoring Plaintiffs’ credit, monitoring their financial accounts.

1 29. At present, the damages have not fully developed because Defendants have not
2 disclosed their actions, but are currently no more than \$70,000.

3 30. Plaintiffs also demand an immediate restoration of their data and injunctive relief,
4 which has been deprived.

5 **Defendants Failed to Comply with Regulatory Guidance and Meet Consumers' Expectations**

6 31. Federal agencies have issued recommendations and guidelines to temper data
7 breaches and the resulting harm to individuals and financial institutions. For example, the FTC has
8 issued numerous guides for business highlighting the importance of reasonable data security
9 practices. According to the FTC, the need for data security should be factored into all business
10 decision-making.

11 32. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*
12 *for Business*, which established guidelines for fundamental data security principles and practices for
13 business. Among other things, the guidelines note businesses should protect the personal customer
14 information that they keep; properly dispose of personal information that is no longer needed;
15 encrypt information stored on computer networks; understand their network's vulnerabilities; and
16 implement policies to correct security problems. The guidelines also recommend that businesses use
17 an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for
18 activity indicating someone is attempting to hack the system; watch for large amounts of data being
19 transmitted from the system; and have a response plan ready in the event of a breach.

20 33. Additionally, the FTC recommends that companies limit access to sensitive data;
21 require complex passwords to be used on networks; use industry-tested methods for security;
22 monitor for suspicious activity on the network; and verify that third-party service providers have
23 implemented reasonable security measures.

24 34. The FTC has brought enforcement actions against businesses for failing to adequately
25 and reasonably protect customer information, treating the failure to employ reasonable and
26 appropriate measures to protect against unauthorized access to confidential consumer data as an
27 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.
28

1 Orders resulting from these actions further clarify the measures businesses must take to meet their
2 data security obligations.

3 35. In this case, Defendants were fully aware of their obligation to use reasonable
4 measures to protect the PII of Plaintiffs, acknowledging as much in its own privacy policies. But
5 despite understanding the consequences of inadequate data security, Defendants failed to comply
6 with industry standard data security requirements.

7 36. Defendants' failure to employ reasonable and appropriate measures to protect against
8 unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of
9 the FTC Act, 15 U.S.C. § 45 and various state consumer protection and data breach statutes.

10 **Effect of the Data Breach**

11 37. Defendants' failure to keep Plaintiffs' PII secure has severe ramifications. Given the
12 sensitive nature of the PII stolen in the Data Breach, cyber criminals have the ability to commit
13 identity theft and other identity-related fraud against Plaintiffs now and into the indefinite future.

14 38. The information stolen from Defendants included usernames and passwords—PII that
15 is highly valued among cyber thieves and criminals on the Dark Web. For example, Apple ID
16 usernames and passwords were sold on average for \$15.39 each on the Dark Web, making them the
17 most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for
18 eBay (\$12), Amazon (≤\$10), and Walmart (≤\$10) fetch similar amounts. Consumers often reuse
19 passwords. By unlawfully obtaining this information, cyber criminals can use these credentials to
20 access other services beyond that which was hacked.

21 39. Other information stored on Defendants' databases that were compromised in the
22 Data Breach can fetch far more on the Dark Web. Stolen medical records “can fetch up to \$350 on
23 the dark web.”

24 40. PII also has significant monetary value in part because criminals continue their efforts
25 to obtain this data. In other words, if any additional breach of sensitive data did not have
26 incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such
27 additional data over time. Instead, just the opposite has occurred.

1 41. The value of PII is key to unlocking many parts of the financial sector for consumers.
2 Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a
3 job depends on the integrity of their PII. Similarly, the businesses that request (or require) consumers
4 to share their PII as part of a commercial transaction do so with the expectation that its integrity has
5 not been compromised.

6 42. Annual monetary losses for victims of identity theft are in the billions of dollars. In
7 2017, fraudsters stole \$16.8 billion from consumers in the United States, which includes \$5.1 billion
8 stolen through bank account take-overs.

9 43. The annual cost of identity theft is even higher. McAfee and the Center for Strategic
10 and International Studies estimates that the likely annual cost to the global economy from
11 cybercrime is \$445 billion a year.

12 44. Over 1 million minor children were victims of fraud or identity theft in 2017, and
13 two-thirds of those victims were under the age of seven.

14 45. Data thieves are also more likely to target minors' PII and to use that PII once it is
15 stolen. In 2017, "[a]mong notified breach victims . . . 39 percent of minors became victims of fraud,
16 versus 19 percent of adults."

17 46. Criminals make use of minors' PII to open accounts or new lines of credit that may
18 not be noticed by the minor; and to create "synthetic identities" using a combination of real and
19 fictitious information which again, the minor may not realize was stolen. Because minors do not
20 regularly monitor their bank accounts (if they have them) or their credit reports, data thieves are
21 more likely to make unrestricted use of this information for longer periods of time than they would
22 for adult victims.

23 47. Minors also generally are less likely to receive notice from the company responsible
24 for the data breach or to even realize that a thief has made fraudulent use of their information in
25 other ways – such as creating a new identity for the purposes of accessing government benefits,
26 healthcare, or employment. Minors often "won't find out that their identity has been stolen until
27 they apply for their first credit card or college loan."
28

1 48. Reimbursing a consumer for a financial loss due to fraud does not make that
2 individual whole again. On the contrary, in addition to the irreparable damage that may result from
3 the theft of PII, identity theft victims must spend numerous hours and their own money repairing the
4 impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice
5 Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up
6 the issues" and resolving the consequences of fraud in 2014.

7 49. Even before the occurrence of identity theft, victims may spend valuable time and
8 suffer from the emotional toll of a data breach. Here, Plaintiff Gupta has already spent
9 approximately two hours investigating the Data Breach after receiving notice from ABC, including
10 independent online research regarding the scope of the breach and communicating with ABC
11 regarding the breach. Plaintiffs will continue to expend time monitoring credit and other identity-
12 related information.

13 50. The impact of identity theft can have ripple effects, which can adversely affect the
14 future financial trajectories of victims' lives. For example, the Identity Theft Resource Center
15 reports that respondents to their surveys in 2013-2016 described that the identity theft they
16 experienced affected their ability to get credit cards and obtain loans, such as student loans or
17 mortgages. For some victims, this could mean the difference between going to college or not,
18 becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-
19 interest loan.

20 51. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims.
21 The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by
22 victims of identity theft:

- 23 • 75% of respondents reported feeling severely distressed;
- 24 • 67% reported anxiety;
- 25 • 66% reported feelings of fear related to personal financial safety;
- 26 • 37% reported fearing for the financial safety of family members;
- 27 • 24% reported fear for their physical safety;
- 28 • 15.2% reported a relationship ended or was severely and negatively

○ impacted by the identity theft; and

- 7% reported feeling suicidal.

52. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.

53. There may also be a significant time lag between when PII is stolen and when it is actually misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

54. The risk of identity theft is particularly acute where detailed personal information is stolen, such as the PII that was compromised in the Data Breach.

55. As the result of the Data Breach, Plaintiffs have suffered or will suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

- identity theft and fraud resulting from theft of their PII;
- costs associated with the detection and prevention of identity theft and unauthorized use of their online accounts, including financial accounts;
- losing the inherent value of their PII;

- d. losing the value of Defendants' explicit and implicit promises of adequate data security;
- e. costs associated with purchasing credit monitoring and identity theft protection services;
- f. unauthorized access to and misuse of their online accounts;
- g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;
- h. lowered credit scores resulting from credit inquiries following fraudulent activities;
- i. costs associated with time spent and the loss of productivity or enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, addressing other varied instances of identity theft – such as credit cards, bank accounts, loans, government benefits, and other services procured using the stolen PII, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, updating login information for online accounts sharing the same login credentials as were compromised in the Data Breach, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;
- j. the continued imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or more unauthorized third parties; and
- k. continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs.

56. Additionally, Plaintiffs place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.

57. The cost of hosting or processing consumers', parents', and guardians PII on or through Defendants' databases and systems includes things such as the actual cost of the servers and employee hours needed to process said transactions. One component of the cost of using these services is the explicit and implicit promises Defendants made to protect consumers', parents', and guardians' PII. Because of the value consumers and their parents and guardians place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers, parents, guardians, and school districts did not value their data security and privacy, companies like Defendants would have no reason to tout their data security efforts to their actual and potential customers.

58. Had the victims of the Data Breach including Plaintiffs known the truth about Defendants' data security practices - that Defendants would not adequately protect and store their data—they would have demanded that their school districts not store their PII on Defendants' databases or process it through Defendants' systems.

59. Plaintiffs are at an imminent risk of fraud, criminal misuse of their PII, and identity theft for years to come as result of the data breach and Defendants' deceptive and unconscionable conduct.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Intrusion Upon Seclusion

(Brought on Behalf of Plaintiffs)

60. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

1 61. California adheres to Restatement (Second) of Torts, § 652B with no material
2 variation.

3 62. “One who intentionally intrudes, physically or otherwise, upon the solitude or
4 seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion
5 of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement
6 (Second) of Torts, § 652B.

7 63. Plaintiffs have reasonable expectations of privacy in their records and PII.

8 64. The reasonableness of such expectations of privacy is supported by Defendants’
9 unique position to store Plaintiffs’ business and personal data.

10 65. Defendants intentionally intruded on and into Plaintiffs’ solitude, seclusion, or private
11 affairs by constructing an inadequate system to store data of consumers and their parents.

12 66. These intrusions are highly offensive to a reasonable person. This is evidenced by,
13 *inter alia*, countless consumer surveys, studies, and op-eds decrying the data breach and tracking of
14 children, centuries of common law, state and federal statutes and regulations, legislative
15 commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and
16 scholarly literature on consumers’ reasonable expectations. Further, the extent of the intrusion
17 cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs’ personal
18 information with potentially countless third-parties, known and unknown, for undisclosed and
19 potentially unknowable purposes, in perpetuity.

20 67. Defendants’ intrusion into the sacrosanct relationship between parent and child and
21 subsequent exploitation of children’s special vulnerabilities online through lax data and
22 cybersecurity practices contributes to the highly offensive nature of Defendants’ activities.

23 68. Plaintiffs were harmed by the intrusion into their private affairs as detailed throughout
24 this Complaint.

25 69. Defendants’ actions and conduct complained of herein were a substantial factor in
26 causing the harm suffered by Plaintiffs.

70. As a result of Defendants' actions, Plaintiffs seek injunctive relief, in the form of Defendants' cessation of tracking practices in violation of state law, and restoring access to Plaintiffs data.

71. As a result of Defendants' actions, Plaintiffs seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs seek punitive damages because Defendants' actions—which were malicious, oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

72. Plaintiffs seek restitution for the unjust enrichment obtained by Defendants' as a result of the Data Breach.

SECOND CAUSE OF ACTION

California Constitutional Right to Privacy

(Brought on Behalf of Plaintiffs)

73. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

74. Plaintiffs have reasonable expectations of privacy in their files with the school.

75. Defendants recklessly intruded on and into Plaintiffs' solitude, seclusion, right of privacy, or private affairs by intentionally designing the computer systems and databases in a manner subject to, and vulnerable to a cybersecurity attack.

76. These intrusions are highly offensive to a reasonable person, because they disclosed sensitive and confidential information about children, constituting an egregious breach of social norms. This is evidenced by, *inter alia*, countless consumer surveys, studies, and op-eds decrying the online tracking of children, centuries of common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, and scholarly literature on consumers' reasonable expectations. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity.

77. Defendants' intrusion into the sacred relationship between parent and child and subsequent exploitation of children's special vulnerabilities online also contributes to the highly offensive nature of Defendants' activities.

78. Plaintiffs were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

79. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs.

80. As a result of Defendants' actions, Plaintiffs seek injunctive relief, in the form of Defendants' restoration of all data. As a result of Defendants' actions, Plaintiffs seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs seek punitive damages because Defendants' actions - which were malicious, oppressive, willful - were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

THIRD CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT

(Cal. Civ. Code § 56, *et seq.*)

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

81. The preceding factual statements and allegations are incorporated by reference.

82. Section 56.10(a) of the California Civil Code (CMIA) provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

83. At all relevant times, Defendants were contractors and/or health care providers because they had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." Cal. Civ. Code § 56.06(a).

1 84. At all relevant times. Defendants collected, stored, managed, and transmitted
2 Plaintiffs' PII/PHI.

3 85. The CMIA requires Defendants to implement and maintain standards of
4 confidentiality with respect to all individually identifiable PHI disclosed to them, and maintained by
5 them. Specifically, California Civil Code § 56.10(a) prohibits Defendants from disclosing Plaintiffs'
6 PHI without first obtaining their authorization to do so.

7 86. Section 56.11 of the California Civil Code specifies the manner in which
8 authorization must be obtained before PHI is released. Defendants, however, failed to obtain let
9 alone, proper authorization - from Plaintiffs before causing the systems to be exposed and subject to
10 data breach. Defendants also failed to identify, implement, maintain and monitor the proper data
11 security measures, policies, procedures, protocols, and software and hardware systems to safeguard
12 and protect Plaintiffs' PHI as required by California law. As a direct and proximate result of
13 Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' PHI was
14 disclosed. By disclosing Plaintiffs' PHI without their written authorization. Defendants violated
15 California Civil Code § 56, *et seq.*, and their legal duty to protect the confidentiality of such
16 information.

17 87. Defendants also violated Sections 56.06 and 56.101 of the California CMIA, which
18 prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or
19 disposal of confidential PHI. As a direct and proximate result of Defendants' wrongful actions,
20 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,
21 Plaintiffs' confidential PHI was viewed, released and disclosed without their authorization by
22 unauthorized persons.

23 88. As a direct and proximate result of Defendants' above-described wrongful actions,
24 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,
25 and violation of the CMIA, Plaintiffs have suffered (and will continue to suffer) economic damages
26 and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the
27 continuing increased risk of identity theft, identity fraud and medical fraud - risks justifying
28 expenditures for protective and remedial services for which she is entitled to compensation, (ii)

1 invasion of privacy, (iii) breach of the confidentiality of her PII/PHI, (iv) statutory damages under
 2 the California CMIA, (v) deprivation of the value of her PII/PHI, for which there is a well-
 3 established national and international market, and/or (vi) the financial and temporal cost of
 4 monitoring her credit, monitoring their financial accounts, and mitigating Plaintiffs' damage and
 5 inconvenience damages.

6 89. As a direct and proximate result of Defendants' above-described wrongful actions,
 7 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
 8 and its violation of the CMIA, Plaintiffs also are entitled to (i) injunctive relief, (ii) punitive damages
 9 of up to \$3,000 per Plaintiffs, and (iii) attorneys' fees, litigation expenses and court costs under
 10 California Civil Code § 56.35.

11 **FOURTH CAUSE OF ACTION**

12 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW**

13 **(Cal. Bus. & Prof. Code § 17200, et seq.)**

14 **(On Behalf of Plaintiffs against all Defendants and DOES 1-100)**

15 90. Plaintiffs re-allege and incorporate by reference herein each and every allegation
 16 contained herein above as though fully set forth and brought in this cause of action.

17 91. The California Unfair Competition Law, Cal Bus. & Prof. Code § 17200, *et seq.*,
 18 prohibits any "unlawful, fraudulent" or "unfair" business act or practice and any false or misleading
 19 advertising, as those terms are defined by the UCL and relevant case law. By virtue of their above-
 20 described wrongful actions, inaction, omissions, and want of ordinary care that directly and
 21 proximately caused the Data Breach, Defendants engaged in unlawful, unfair, and fraudulent
 22 practices within the meaning, and in violation of, the UCL.

23 92. In the course of conducting its business. Defendants committed "unlawful business
 24 practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee,
 25 manage, monitor and audit appropriate data security processes, controls, policies, procedures,
 26 protocols, and software and hardware systems to safeguard and protect Plaintiffs' PII/PHI, and
 27 violating the statutory and common law alleged herein in the process, including, *inter alia*, the
 28 California CMIA, the California CRA, and the California IPA. Plaintiffs reserve the right to allege

1 other violations of law by Defendants constituting other unlawful business acts or practices.
2 Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are
3 ongoing and continue to this date.

4 93. Defendants also violated the UCL by failing to timely notify Plaintiffs regarding the
5 unauthorized release (and/or threats of unauthorized release) and disclosure of their PII/PHI. If
6 Plaintiffs had been notified in an appropriate fashion, they could have taken precautions to safeguard
7 and protect their PII/PHI, medical information, and identities.

8 94. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary
9 care, misrepresentations, practices, and non-disclosures also constitute "unfair business acts and
10 practices" in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to
11 consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. The
12 gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such
13 conduct. There were reasonably available alternatives to further Defendants' legitimate business
14 interests other than engaging in the above-described wrongful conduct.

15 95. The UCL also prohibits any "fraudulent business act or practice." Defendants' above-
16 described claims, nondisclosures and misleading statements were false, misleading and likely to
17 deceive the consuming public in violation of the UCL.

18 96. As a direct and proximate result of Defendants' above-described wrongful actions,
19 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
20 and their violations of the UCL, Plaintiffs have suffered (and will continue to suffer) economic
21 damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and
22 the continuing increased risk of identity theft, risks justifying expenditures for protective and
23 remedial identity fraud and medical fraud services for which she is entitled to compensation, (ii)
24 invasion of privacy, (iii) breach of the confidentiality of her PII/PHI, (iv) statutory damages under
25 the California CMIA, (v) deprivation of the value of her PII/PHI, for which there is a well-
26 established national and international market, and/or (vi) the financial and temporal cost of
27 monitoring her credit, monitoring her financial accounts, and mitigating her damages.
28

97. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, also seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to them, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203. In addition, Plaintiffs demand immediate restoration to their data.

FIFTH CAUSE OF ACTION

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

99. To ensure that personal information about California residents is protected, the California Legislature enacted the Customer Records Act, California Civil Code § 1798.81.5, which requires that any business that “owns licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”

101. Under California Civil Code § 1798.82, any business that obtains and retains PII/PHI must promptly and “in the most expedient time possible and without unreasonable delay” disclose any Data Breach involving such retained data.

1 audit appropriate data security processes, controls, policies, procedures, protocols, and software and
2 hardware systems to safeguard and protect Plaintiffs' PII/PHI.

3 103. Defendants also unreasonably delayed and failed to disclose the Data Breach (and
4 threat of the data breach) to Plaintiffs in the most expedient time possible and without unreasonable
5 delay when they knew, or reasonably believed, Plaintiffs' PII/PHI had been wrongfully disclosed to
6 an unauthorized person or persons.

7 104. As a direct and proximate result of Defendants' above-described wrongful actions,
8 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach
9 and its violations of the California CRA, Plaintiffs have suffered (and will continue to suffer)
10 economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent,
11 immediate and the continuing increased risk of identity theft, identity fraud and medical fraud - risks
12 Justifying expenditures for protective and remedial services for which she is entitled to
13 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of her PII/PHI, (iv) statutory
14 damages under the California CMIA, (v) deprivation of the value of her PII/PHI, for which there is a
15 well-established national and international market, and/or (vi) the financial and temporal cost of
16 monitoring her credit, monitoring her financial accounts, and mitigating her damages.

17 105. Plaintiff is also entitled to injunctive relief under California Civil Code Section
18 1798.84(e).

19 **SIXTH CAUSE OF ACTION**

20 **VIOLATION OF THE CALIFORNIA INFORMATION PRACTICES ACT**

21 **(Cal. Civ. Code §§ 1798, *et seq.*)**

22 **(On Behalf of Plaintiffs against all Defendants and DOES 1-100)**

23 106. Plaintiffs re-allege and incorporate by reference herein each and every allegation
24 contained herein above as though fully set forth and brought in this cause of action.

25 107. Pursuant to the California Information Practices Act of 1977, California Civil Code §
26 1798.21, an agency is required "to establish appropriate and reasonable administrative, technical,
27 and physical safeguards to ensure compliance with provisions of this chapter, to ensure the security
28

1 and confidentiality of records, and to protect against anticipated threats or hazards to their security or
2 integrity which could result in any injury.”

3 108. As described above. Defendants failed to implement and maintain reasonable security
4 procedures and practices to protect the Plaintiffs’ PII/PHI, and thereby violated the California IPA.

5 109. Under California Civil Code § 1798.29, any agency that obtains and retains PII/PHI
6 must promptly and “in the most expedient time possible and without unreasonable delay” disclose
7 any Data Breach involving such retained data.

8 110. By its above-described wrongful actions, inaction, omissions, and want of ordinary
9 care. Defendants failed to design, adopt, implement, control, direct, oversee, manage, monitor and
10 audit appropriate data security processes, controls, policies, procedures, protocols, and software and
11 hardware systems to safeguard and protect Plaintiffs PII/PHI.

12 111. Defendants also unreasonably delayed and failed to disclose the Data Breach to
13 Plaintiffs in the most expedient time possible and without unreasonable delay when they knew, or
14 reasonably believed. Plaintiffs’ PII/PHI had been wrongfully disclosed to an unauthorized person or
15 persons.

16 SEVENTH CAUSE OF ACTION

17 BREACH OF CONFIDENTIALITY

18 (On Behalf of Plaintiffs against all Defendants and DOES 1-100)

19 112. Plaintiffs re-allege and incorporate by reference herein each and every allegation
20 contained herein above as though fully set forth and brought in this cause of action.

21 113. Plaintiffs’ unique, personal, and private PII/PHI in Defendants’ possession, custody,
22 and control was (and continues to be) highly confidential.

23 114. Defendants breached the confidentiality of Plaintiffs’ PII/PHI by failing to identify,
24 implement, maintain and monitor appropriate data security measures, policies, procedures, protocols,
25 and/ software and hardware systems to ensure the security and confidentiality of Plaintiffs’ PII/PHI,
26 and wrongfully releasing and disclosing their PII/PHI without authorization, as described above.

27 115. Had Defendants not engaged in the above-described wrongful actions, inaction and
28 omissions, the Data Breach never would have occurred and Plaintiffs’ PII/PHI would not have been

1 wrongfully released, disclosed, compromised, disseminated to the world, and wrongfully used.
2 Defendants' wrongful conduct constitutes (and continues to constitute) the tort of breach of
3 confidentiality at California common law.

4 116. As a direct and proximate result of Defendants' above-described wrongful actions,
5 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,
6 Plaintiffs have suffered (and will continue to suffer) economic damages and other injury and actual
7 harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of
8 identity theft, identity fraud and medical fraud - risks justifying expenditures for protective and
9 remedial services for which she is entitled to compensation, (ii) invasion of privacy, (iii) breach of
10 the confidentiality of her PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation
11 of the value of her PII/PHI, for which there is a well-established national and international market,
12 and/or (vi) the financial and temporal cost of monitoring her credit, monitoring her financial
13 accounts, and mitigating her damages.

14 **EIGHTH CAUSE OF ACTION**

15 **INVASION OF PRIVACY**

16 **(On Behalf of Plaintiffs against all Defendants and DOES 1-100)**

17 117. Defendants invaded Plaintiffs Members' right to privacy by allowing the
18 unauthorized access to the information of Plaintiffs and negligently maintaining the confidentiality
19 of the information of Plaintiffs, as set forth above. The intrusion was offensive and objectionable to
20 Plaintiff, and to a reasonable person of ordinary sensibilities in that the personal medical information
21 that

22 118. Defendants obtained was disclosed by Defendants without prior written authorization
23 of Plaintiffs.

24 119. The intrusion was into a place or thing which was private and is entitled to be private,
25 in that Plaintiffs' personal medical information provided to Defendants as patients of Defendants
26 were made privately, and was intended to be kept confidential and protected from unauthorized
27 disclosure.
28

120. As a proximate result of Defendants' above acts, Plaintiffs' PII/PHI was viewed, printed, distributed, and used by persons without prior written authorization and Plaintiffs suffered general damages in an amount to be determined at trial according to proof Defendants are liable for oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' personal medical information with a willful and conscious disregard of Plaintiffs' right to privacy.

121. Unless and until enjoined, and restrained by order this Court, Defendants' wrongful conduct will continue to cause Plaintiffs great and irreparable injury in that the PII/PHI maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs have no adequate remedy of law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs.

NINTH CAUSE OF ACTION

CONSTRUCTIVE FRAUD

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

122. The preceding factual statements and allegations are incorporated by reference.

123. Defendants, in collecting Plaintiffs' nonpublic, personal, financial, and health information, were therefore entrusted with Plaintiffs' nonpublic personal, financial, and health information and were put in the same confidential and special relationship with Plaintiffs as they had with the companies that provided them with health insurance.

124. Defendants breached their confidential and special relationship with Plaintiffs by failing to adequately secure Plaintiffs' nonpublic personal and financial information from unauthorized users, including cyber thieves who stole the information as described herein.

125. As a direct and proximate result of Defendants' breach, Plaintiffs have been harmed and have suffered, and will continue to suffer, damages and injuries.

TENTH CAUSE OF ACTION

BREACH OF EXPRESS CONTRACT

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

126. The preceding factual statements and allegations are incorporated by reference.

127. Plaintiffs, upon information and belief entered into express contracts with Defendants that include Defendants' promise to protect nonpublic personal information given to Defendants or that Defendants gather on their own, from disclosure. Defendants' promise was incorporated into each of the privacy policies, student manuals, and other enrollment documents issued to Plaintiffs.

128. Plaintiffs performed their obligations under the contracts when they signed up for education and health services.

129. Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was accessed by unauthorized personnel as part of the cyber hacking Incident that occurred in 2022.

130. As a direct and proximate result of the Data Breach, Plaintiffs have been harmed and have suffered, and will continue to suffer, damages and injuries.

ELEVENTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

131. Defendants provided Plaintiffs with an implied contract to protect and keep Plaintiffs' private nonpublic personal, educational, financial and health information when they gathered the information from each of their consumers.

132. Plaintiffs would not have provided their personal or financial and health information to Defendants or their subsidiaries, but for Defendants' implied promises to safeguard and protect Defendants' consumers' nonpublic personal and financial information.

133. Plaintiffs performed their obligations under the implied contract when they provided their private personal, educational, financial, and health information as consumers and were furnished with the services provided by Defendants.

134. Defendants breached the implied contracts with Plaintiffs by failing to protect and keep private the nonpublic personal and financial information provided to them about Plaintiffs.

135. As a direct and proximate result of Defendants' breach of their implied contracts, Plaintiffs have been harmed and have suffered, and will continue to suffer, damages and injuries.

TWELFTH CAUSE OF ACTION

UNJUST ENRICHMENT

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

136. The preceding factual statements and allegations are incorporated by reference.

137. Plaintiffs conferred a benefit to Defendants in the form of payment taxes for public education.

138. Defendants failed to pay for the benefits provided to them by Plaintiffs by failing to protect and keep private the nonpublic personal financial, educational, and health information with which Plaintiffs entrusted Defendants with.

139. Defendants' failure to pay for the benefits provided to them, *i.e.*, to protect and keep private Plaintiffs' nonpublic personal, financial and health information, was to the detriment of Plaintiffs because it was Plaintiffs' nonpublic personal, financial, and health information that was taken by cyber thieves.

140. As a direct and proximate result of Defendants' failure to pay for the benefits provided to them, Plaintiffs have been harmed and have suffered, and will continue to suffer, damages and injuries, and are entitled to restitution.

THIRTEENTH CAUSE OF ACTION

DECLARATORY RELIEF

(On Behalf of Plaintiffs against all Defendants and DOES 1-100)

141. The preceding factual statements and allegations are incorporated by reference. An actual controversy has arisen in the wake of the data breach regarding Defendants' duties to safeguard and protect Plaintiffs' confidential and sensitive PII/PHI. Defendants' PII/PHI security measures were (and continue to be) woefully inadequate. Defendants dispute these contentions and contend that their security measures are appropriate.

142. Plaintiffs continue to suffer damages, other injury or harm as additional identity theft and identity fraud occurs.

143. Therefore, Plaintiffs request a judicial determination of their rights and duties, to ask the Court to enter a judgment declaring, *inter alia*, (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiffs' confidential and sensitive PII/PHI, and timely notify them

1 about the data breach, (ii) Defendants breached (and continue to breach) such legal duties by failing
 2 to safeguard and protect Plaintiffs' confidential and sensitive PII/PHI, and (iii) Defendants' breach
 3 of their legal duties directly and proximately caused the data breach, and the resulting damages,
 4 injury, or harm suffered by Plaintiffs. A declaration from the court ordering the Defendants to stop
 5 their illegal practices is required.

6 144. The preceding factual statements and allegations are incorporated by reference.

7 **FOURTEENTH CAUSE OF ACTION**

8 **NEGLIGENCE/GROSS NEGLIGENCE/NEGLIGENCE PER SE**

9 **(On Behalf of Plaintiffs against all Defendants and DOES 1-100)**

10 145. The preceding factual statements and allegations are incorporated by reference.

11 146. Defendants, in offering cloud services, knew that Plaintiffs' sensitive PII and data
 12 would be stored or processed by Defendants' systems and databases, including in Defendants
 13 Hosting.

14 147. By collecting, storing, and using this data, Defendants had a duty of care to Plaintiffs
 15 to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting
 16 this PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by
 17 unauthorized persons. More specifically, this duty included, among other things: (a) designing,
 18 maintaining, and testing Defendants' security systems and data storage architecture to ensure that
 19 Plaintiffs' PII was adequately secured and protected; (b) implementing processes that would detect
 20 an unauthorized breach of Defendants' security systems and data storage architecture in a timely
 21 manner; (c) timely acting on all warnings and alerts, including public information, regarding
 22 Defendants' security vulnerabilities and potential compromise of the PII of Plaintiffs; (d)
 23 maintaining data security measures consistent with industry standards and applicable state and
 24 federal law; and (e) timely and adequately informing Plaintiffs if and when a data breach occurred
 25 notwithstanding undertaking (a) through (d) above.

26 148. Defendants had common law duties to prevent foreseeable harm to Plaintiffs. These
 27 duties existed because Plaintiffs were the foreseeable and probable victims of any inadequate
 28 security practices. In fact, not only was it foreseeable that Plaintiffs would be harmed by the failure

1 to protect their PII because hackers routinely attempt to steal such information and use it for
2 nefarious purposes, Defendants knew that it was more likely than not Plaintiffs would be harmed by
3 such theft.

4 149. Defendants had a duty to monitor, supervise, control, or otherwise provide oversight
5 to safeguard the PII that was collected, stored, and processed by Defendants computer systems.

6 150. Defendants' duties to use reasonable security measures also arose as a result of the
7 special relationship that existed between Defendants, on the one hand, and Plaintiffs, on the other
8 hand. The special relationship arose because Plaintiffs entrusted Defendants with their PII by virtue
9 of their participation in all aspects of school life. Defendants alone could have ensured that its
10 security systems and data storage architecture were sufficient to prevent or minimize the Data
11 Breach.

12 151. Defendants' duties to use reasonable data security measures also arose under Section
13 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . .
14 practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair
15 practice of failing to use reasonable measures to protect PII. Various FTC publications and data
16 security breach orders further form the basis of Defendants' duties. In addition, individual states
17 have enacted statutes based upon the FTC Act that also created a duty.³

18 152. Defendants knew or should have known that their computer systems and data storage
19 architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of
20 stealing and misusing confidential PII and business data.

21 153. Defendants knew or should have known that a breach of their systems and data
22 storage architecture would inflict damages upon Plaintiffs, and Defendants was therefore charged
23 with a duty to adequately protect this critically sensitive information.

24 154. Defendants breached the duties it owed to Plaintiffs described above. Defendants
25 breached these duties by, among other things, failing to: (a) exercise reasonable care and implement
26 adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs; (b) detect
27

28 ³ While the FTC Act is referred to herein, none of the causes of action rely on any Federal Cause of action, but rely exclusively on California causes of action.

1 the breach while it was ongoing; and (c) maintain security systems consistent with industry
2 standards.

3 155. Defendants also failed to exercise reasonable care when it falsely conveyed
4 information to its customer and apprise them of details.

5 156. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs,
6 Plaintiffs' PII would not have been compromised.

7 157. As a direct and proximate result of Defendants' negligence, Plaintiffs have been
8 injured and are entitled to damages in an amount to be proven at trial but no more than \$70,000 at
9 present. Such injuries include one or more of the following: ongoing, imminent, certainly impending
10 threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic
11 harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic
12 harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the
13 compromised PII on the black market; mitigation expenses and time spent on credit monitoring,
14 identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach
15 investigating the nature of the Data Breach not fully disclosed by Defendants, reviewing bank
16 statements, payment card statements, and credit reports; expenses and time spent initiating fraud
17 alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their
18 bargains and overcharges for services; and other economic and non-economic harm.

19 **FIFTEENTH CAUSE OF ACTION**

20 **CALIFORNIA CONSUMER PRIVACY ACT**

21 **Cal. Civ. Code §§ 1798.100 *et seq.***

22 **(On Behalf of Plaintiffs against all Defendants and DOES 1-100)**

23 158. The preceding factual statements and allegations are incorporated by reference.

24 159. Plaintiffs are "consumer[s]" as that term is defined in Cal. Civ. Code. § 1798.140(g).
25 Rackspace is considered a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c).

26 160. Plaintiffs' PII is "nonencrypted and nonredacted personal information" as that term is
27 used in Cal. Civ. Code § 1798.150(a)(1). The Data Breach constitutes "an unauthorized access and
28 exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1).

161. Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiffs to protect said PII.

162. Defendants breached the duty they owed to Plaintiffs described above by among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

163. Defendants' breach of the duty they owed to Plaintiffs described above was the direct and proximate cause of the Data Breach. As a result, Plaintiffs members suffered damages, as described above and as will be proven at trial.

164. Plaintiffs seek injunctive relief in the form of an order enjoining Defendants from continuing the practices that constituted their breach of the duty owed to Plaintiffs as described above, and to restoring the data belonging to Plaintiffs. Concurrently with the filing of this Complaint, Plaintiffs are serving a letter of notice on Rackspace pursuant to Cal. Civ. Code § 1798.150(b) and anticipate amending this Complaint to seek statutory damages upon receipt of a written statement from Rackspace in response to that letter of notice.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court enter judgment in their favor and against Defendants as follows:


- 1) For injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs, including but not limited to an order:
 - a) Restoring and returning Plaintiffs' data to them;
 - b) Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - c) Requiring Defendants to protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 - d) Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' PII;

- e) Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - f) Requiring Defendants to audit, test, and train its personnel regarding any new or modified procedures;
 - g) Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;
 - h) Requiring Defendants to conduct regular database scanning and security checks;
 - i) Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs;
 - j) Requiring Defendants to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
 - k) Requiring Defendants to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - l) Requiring Defendants to meaningfully educate consumers about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;
 - m) Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from its servers, as well as programs sufficient to protect infiltration of school districts' local servers connected to Defendants' systems; and
 - n) Requiring Defendants to provide ten years of identity theft and fraud protection services to Plaintiffs.
- 2) For an award of compensatory, consequential, and general damages, including nominal

- 1 damages, as allowed by law in an amount to be determined but no more than \$70,000 (until
2 more information is known about the extent of the “security incident”);
- 3 3) For an award of statutory damages and punitive damages, as allowed by law in an amount to
4 be determined, but such damages collectively, of no more than \$70,000;
- 5 4) For an award of restitution or disgorgement of amounts paid to Rackspace, in an amount to
6 be determined;
- 7 5) For an award of attorneys’ fees, costs, and litigation expenses, as allowed by law;
- 8 6) For prejudgment interest on all amounts awarded; and
- 9 7) Such other and further relief as the Court may deem just and proper.

10
11 Dated: December 9, 2022

Respectfully submitted,

12
13 
14 By: _____

15 Blake J. Lindemann
16 California Bar No. 255747
17 E-mail: blake@lawbl.com
18 Donna R. Dishbak
19 California Bar No. 259311
20 E-mail: donna@lawbl.com
21 **LINDEMANN LAW FIRM, APC**
22 433 N. Camden Drive, 4th Floor
23 Beverly Hills, CA 90210
24 Telephone No: 310-279-5269
25 Facsimile No: 310-300-0267


26
27 *Attorneys for Plaintiffs*
28

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all issues so triable.

Dated: December 9, 2022

Respectfully submitted,

By:  _____

Blake J. Lindemann

California Bar No. 255747

E-mail: blake@lawbl.com

Donna R. Dishbak

California Bar No. 259311

E-mail: donna@lawbl.com

LINDEMANN LAW FIRM, APC

433 N. Camden Drive, 4th Floor

Beverly Hills, CA 90210

Telephone No: 310-279-5269

Facsimile No: 310-300-0267

Attorneys for Plaintiffs

LINDEMANN LAW FIRM, APC
433 N. CAMDEN DRIVE, 4TH FLOOR
BEVERLY HILLS, CA 90210